STATEMENT OF THE CLAIMS

1 - 23 (previously cancelled)

24 - 42 (cancelled)

43. (new) A method of permitting authentication of data comprising:

(a) storing copies of a plurality of data items;

(b) generating a first data file comprising a respective hash value of each said plurality of stored data items;

(c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items;

(d) transmitting said single hash value to a remote location, via an information technology communications network;

(e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value;

(f) generating a hash value for said second data file; and

(g) publishing said hash value for said second data file in a journal for authenticating said second data file.

44. (new) A method according to claim 43, further comprising:

(h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in (g).

45. (new) A method according to claim 43, wherein:

said first data file is generated in (b) at the end of a predetermined time period.

46. (new) A method according to claim 43, wherein:

said first data file contains at least one identifier selected from the group consisting of a file name, a path name, a file size and a time stamp.

47. (new) A method according to claim 43, further comprising:

(i) generating a hash value for a selected one of the data items;

(j) digitally signing and encrypting said hash value with a secret identifier associated with the first user;

(k) transmitting to a second user said encrypted hash value;

(l) receiving and storing said transmitted encrypted hash value for audit purposes; and generating a further hash value for said received encrypted hash value;

(m) encrypting the further hash value with a private identifier associated with a second user;

(n) encrypting the encrypted further hash value with a public identifier associated with the first user; and

(o) returning the encrypted further hash value of (n) to the first user.

48. (new) A method according to claim 47, further comprising:

(p) receiving said encrypted further hash value of (n) returned to the first user in step (o);

(q) decrypting said received encrypted data with the private identifier associated with said second user and the public identifier associated with said first user to derive a hash value therefrom; and

(r) comparing the hash value derived in (q) with the hash value generated in (j) to confirm digital identity of the second user.

49. (new) A method according to claim 48, further comprising:

(s) in response to the comparing of (r) confirming digital identity of the second user, encrypting the secret identifier associated with the first user and transmitting to the second user the encrypted secret identifier associated with the first user for decryption and subsequent use in decrypting said encrypted data item of (j).

50. (new) A method according to claim 49, further comprising:

(t) in response to the comparing of (r) failing to confirm digital identity of the second user, denying the second user access to the encrypted data item of (j).

51. (new) A method according to claim 50, wherein:

in (t), the second user is denied access to the encrypted data item of (j) by omission of transmitting to the second user the encrypted secret identifier associated with the first user.

52. (new) A method according to claim 49, wherein:

the encrypted secret identifier generated in (s) is encrypted with a key that is obtained through a transaction between said second user and a third party.

53. (new) A method according to claim 52, wherein:

said transaction between said second user and said third party is recorded and time stamped by said third party.

54. (new) A method of transmitting data between a first user and a second user via an information technology communications network, comprising the steps of:

generating a first hash value for a selected one of the data items;

digitally signing and encrypting said first hash value with a secret identifier associated with the first user;

transmitting to a second user said encrypted first hash value;

receiving and storing said transmitted encrypted first hash value for audit purposes and generating a second hash value for said received encrypted first hash value;

encrypting the second hash value with a private identifier associated with a second user and a public identifier associated with the first user; and

returning the encrypted second hash value to the first user.

55. (new) A method according to claim 54, further comprising:

receiving said encrypted second hash value returned to the first user;

decrypting said received encrypted second hash value with the private identifier associated with said second user and the public identifier associated with said first user to derive a hash value therefrom; and

comparing the derived hash value derived with the second hash value generated for said received encrypted first hash value to confirm digital identity of the second user.

56. (new) A method according to claim 55, further comprising:

in response to the comparing of confirming digital identity of the second user, encrypting the secret identifier associated with the first user and transmitting to the second user the encrypted secret identifier associated with the first user for decryption and subsequent use in decrypting said encrypted first hash value.

57. (new) A method according to claim 55, further comprising:

in response to the comparing of failing to confirm digital identity of the second user, denying the second user access to the encrypted first hash value.

58. (new) A method according to claim 57, wherein:

the second user is denied access to the encrypted first hash value by omission of transmitting to the second user the encrypted secret identifier associated with the first user.

59. (new) A method according to claim 58, wherein:

the secret identifier is encrypted with a key that is obtained through transactions between said second user and a third party.

60. (new) A method according to claim 59, wherein:

at least one of said transactions between said second user and said third party is recorded and time stamped by said third party.

61. (new) A method according to claim 54, wherein:

the encrypted first hash value is stored remotely from said first and second end users.

62. (new) A method according to claim 54, wherein:

the encrypted first hash value is stored by a third party.